

Serie Secure Remote Access

Permite la productividad del trabajador móvil y remoto al tiempo que lo protege contra amenazas

La serie Dell SonicWALL Secure Remote Access (SRA) ofrece a los trabajadores móviles y remotos que utilizan teléfonos inteligentes, tabletas o equipos portátiles (sin importar si se trata de un dispositivo personal administrado o no administrado) un acceso rápido, seguro y determinado por políticas a las aplicaciones, los datos y los recursos, sin poner en riesgo la seguridad.

Para los dispositivos móviles, la solución incluye la aplicación intuitiva Dell SonicWALL Mobile Connect que proporciona a los dispositivos iOS, Android, Kindle Fire, Windows y Mac OS X un acceso seguro a los recursos de red permitidos, incluidos carpetas compartidas, aplicaciones del servidor de cliente, sitios de intranet y correo electrónico.

Los usuarios y los administradores de TI pueden descargar la aplicación Mobile Connect a través de Apple App Store, Google Play y la tienda de Kindle, y los teléfonos inteligentes, las tabletas y los equipos portátiles con Windows 8.1 cuentan con la aplicación Mobile Connect preinstalada. La solución también admite acceso a navegador seguro y sin cliente, incluida compatibilidad con navegadores HTML 5 estándares de la industria y acceso a VPN de cliente ligero para equipos de escritorio y portátiles, incluidos equipos Windows, Mac OS X y Linux.

Para brindar protección frente a acceso no autorizado y malware, el dispositivo de la serie SRA conecta únicamente usuarios autorizados y dispositivos de confianza a los recursos permitidos. Cuando se integra en un firewall de última generación Dell SonicWALL como una Clean VPN, la solución combinada proporciona control de acceso centralizado, protección frente a malware, control de aplicación y filtrado de contenido. La protección multicapa de Clean VPN descifra y descontamina todo el tráfico SSL VPN autorizado antes de que ingrese al entorno de red.

Por qué necesita SRA

La proliferación de dispositivos móviles en el sitio de trabajo ha aumentado la demanda de acceso seguro a aplicaciones, datos y recursos críticos. La posibilidad de brindar ese acceso proporciona importantes beneficios en la productividad de la organización, pero también presenta riesgos significativos.

Por ejemplo, una persona no autorizada puede obtener acceso a los recursos de la compañía utilizando un dispositivo extraviado o robado. El dispositivo móvil de un empleado puede actuar como un medio para infectar la red con malware, o también es posible que redes inalámbricas de terceros intercepten los datos corporativos. Asimismo, también pueden perderse datos comerciales almacenados en los dispositivos si una aplicación personal o un usuario obtienen acceso a los datos sin autorización.

A medida que las organizaciones ya no pueden ejercer influencia sobre la selección de dispositivos y la administración de dispositivos de control, la seguridad de estos dispositivos se torna cada vez más difícil. Las organizaciones deben implementar soluciones que resguarden el acceso a fin de garantizar que solo los usuarios y dispositivos autorizados que cumplen con la política de seguridad obtengan acceso a la red, y que los datos de la compañía en tránsito y almacenados en el dispositivo estén asegurados. Lamentablemente, esto suele involucrar diversas soluciones complejas de proveedores diferentes y eleva considerablemente el costo total de propiedad de la entrega de acceso móvil. Las organizaciones buscan soluciones de acceso móvil sencillas, rentables y seguras que aborden las necesidades de su personal, que cada vez es más móvil.



Beneficios:

- La puerta de enlace de acceso único a todos los recursos de red, a través de aplicación móvil, sin cliente o con clientes web, reduce los gastos de TI y el costo total de propiedad.
- La experiencia de usuario común en todos los sistemas operativos simplifica el uso desde cualquier extremo.
- La aplicación Mobile Connect para iOS, Android, Windows 8.1 y Mac OS X ofrece facilidad de uso para dispositivos móviles.
- La autenticación con reconocimiento del contexto garantiza que solo los usuarios autorizados y los dispositivos móviles confiables puedan acceder.
- Búsqueda segura de archivos de intranet con un solo clic y protección de datos en el dispositivo.
- Las direcciones y el enrutamiento adaptables implementan los métodos de acceso y niveles de seguridad adecuados.
- El asistente de configuración simplifica la implementación.
- Administración eficiente de políticas basadas en objetos para todos los usuarios, grupos, recursos y dispositivos.
- El firewall de aplicación web permite el cumplimiento con PCI.

Acceso rápido, sencillo y determinado por políticas a aplicaciones, datos y recursos críticos, sin poner en riesgo la seguridad.

Características

Puerta de enlace de acceso único para aplicación móvil, sin cliente o clientes web: SRA reduce los costos de TI al permitir que los administradores de red implementen y administren fácilmente una puerta de enlace de acceso seguro que extiende el acceso remoto mediante SSL VPN a los usuarios internos y externos de todos los recursos de red, incluidas aplicaciones basadas en web, cliente/servidor, basadas en host (como escritorio virtual) y de conexión backend (como VoIP). Los dispositivos SRA pueden no tener cliente y acceso de navegador al portal personalizable SRA Workplace, o bien usar aplicaciones móviles o clientes web livianos, lo que reduce los gastos de administración y las llamadas de soporte.

Experiencia de usuario común en todos los sistemas operativos: La tecnología SRA proporciona acceso transparente a los recursos de red desde cualquier dispositivo o entorno de red. Un dispositivo SRA proporciona una puerta de enlace única para el acceso con teléfonos inteligentes, tabletas, equipos de escritorio y portátiles, y una experiencia de usuario común en todos los sistemas operativos (incluidos Windows, Mac OS X, iOS, Android, Kindle y Linux) desde dispositivos administrados y no administrados.

Aplicación Mobile Connect: La aplicación Mobile Connect para dispositivos móviles iOS, Mac OS X, Android, Kindle y Windows 8.1 proporciona a los usuarios un acceso sencillo a nivel de la red para recursos corporativos y académicos en conexiones SSL VPN cifradas. Mobile Connect puede descargarse fácilmente de Apple App Store, Google Play o la tienda de Kindle, y viene integrada en los dispositivos Windows 8.1.

Reconocimiento de contexto: El acceso a la red corporativa solo se otorga luego de que se autentica el usuario y se verifica la integridad del dispositivo móvil.

Protección de los datos almacenados en dispositivos móviles: Los usuarios autenticados pueden navegar y ver los archivos y recursos compartidos de intranet de manera segura desde la aplicación Mobile Connect. Los administradores pueden establecer y reforzar políticas de administración de aplicación móvil.

Direcciones y enrutamiento adaptables: Las direcciones y el enrutamiento adaptables permiten la adaptación dinámica a las redes, lo que elimina los conflictos que suelen experimentar las otras soluciones.

Asistente de configuración: Todos los dispositivos SRA se configuran y se implementan en solo minutos. El asistente de configuración proporciona una experiencia "lista para usar" sencilla e intuitiva para una instalación y una implementación veloces.

Política unificada: La política unificada de SRA proporciona una administración de políticas sencilla y basada en objetos para todos los usuarios, grupos, recursos y dispositivos, al tiempo que refuerza el control granular de acuerdo con la autenticación de usuario y la consulta introducida en el dispositivo.

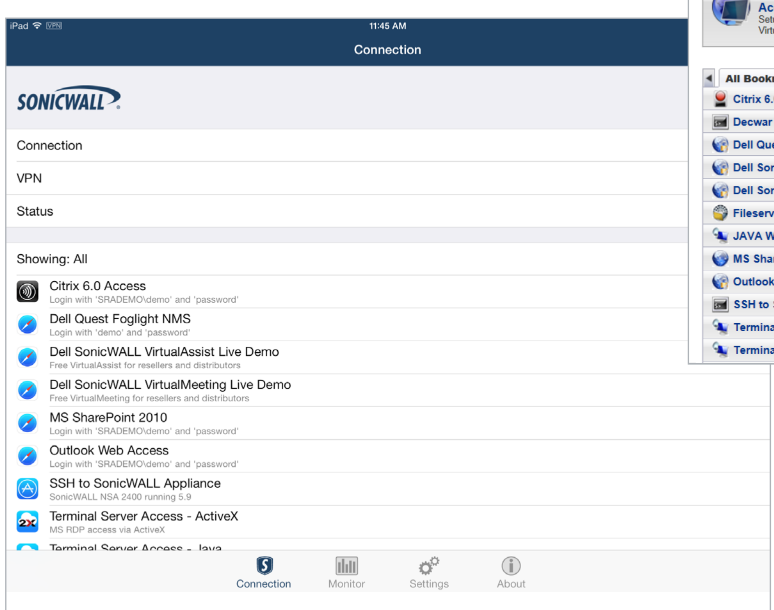


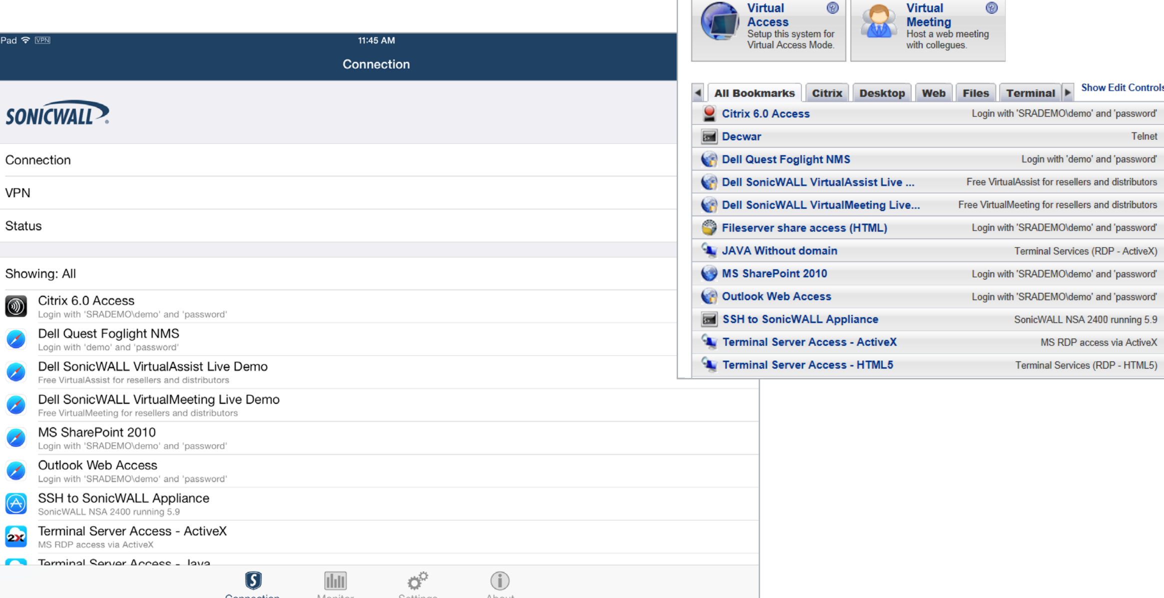


Serie Dell SonicWALL SRA: Acceso en cualquier lugar y momento

Acceso móvil simple y seguro a los recursos

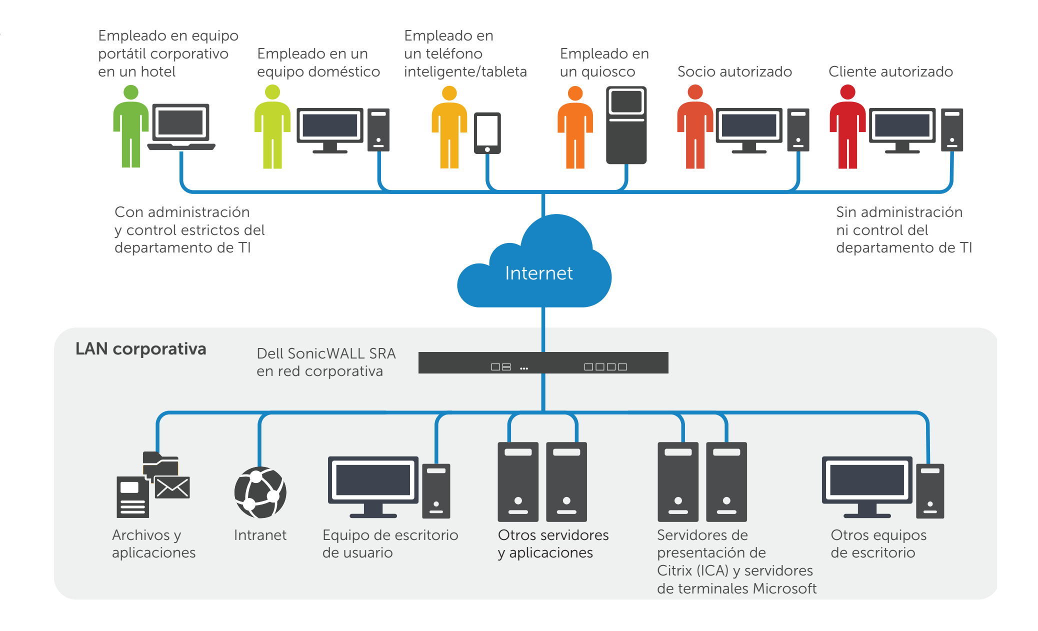
La serie SRA puede utilizarse para ofrecer a los usuarios de Windows, Mac OS X, iOS, Linux, Android y Kindle acceso a una amplia variedad de recursos.





Acceso granular para usuarios autorizados

La serie SRA extiende el acceso móvil y seguro remoto más allá de los empleados administrados hacia los empleados, socios y clientes móviles y remotos no administrados mediante el empleo de controles de acceso granulares y determinados por políticas.





Acceso móvil fácil de usar, rentable y seguro que aborda las necesidades de su personal móvil en crecimiento.

Autenticación con reconocimiento del contexto

La mejor autenticación con reconocimiento del contexto de su clase proporciona acceso únicamente a los dispositivos confiables y los usuarios autorizados. Los dispositivos móviles se prueban para conocer la información de seguridad esencial como el estado de fuga y de raíz, la ID de dispositivo, el estado del certificado y las versiones del sistema operativo antes de otorgar el acceso. Los equipos portátiles y PC también se consultan para identificar la presencia o ausencia del software de seguridad, los certificados de clientes y la ID del dispositivo. Los dispositivos que no cumplan con los requisitos de las políticas no tendrán permitido el acceso a la red y se notificará al usuario acerca del incumplimiento.

Protección de datos almacenados en dispositivos móviles

Los usuarios autenticados de Mobile Connect pueden navegar y ver los archivos y recursos compartidos de intranet de manera segura desde la aplicación Mobile Connect. Los administradores pueden establecer y aplicar la política de administración de aplicaciones móviles para la aplicación Mobile Connect a fin de controlar si los archivos vistos pueden abrirse en otras aplicaciones (iOS 7 y posterior), copiarse al portapapeles, imprimirse o almacenarse en caché de manera segura dentro de la aplicación Mobile Connect. Para iOS 7 y posterior, esto permite a los administradores aislar los datos empresariales de los datos personales almacenados en el dispositivo y reducir el riesgo de pérdida de datos.

Además, si se revocan las credenciales del usuario, el contenido almacenado en la aplicación Mobile Connect está bloqueada y ya no se puede acceder a ella, o verla.

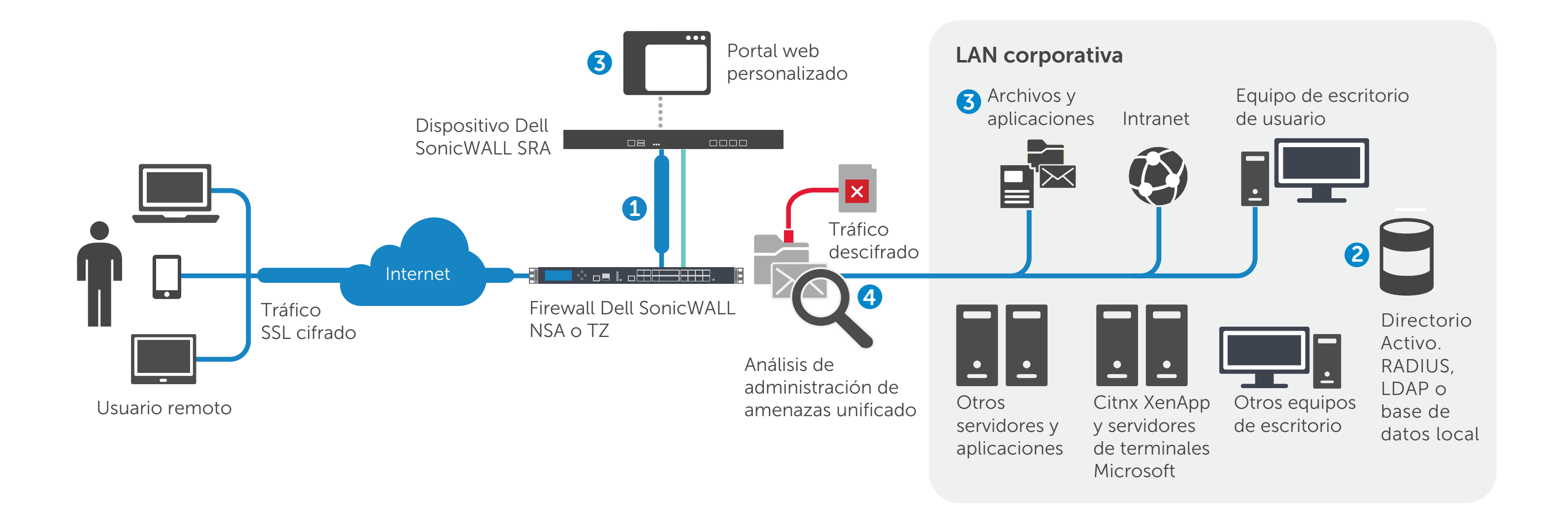
Clean VPN

Cuando se implementa con un firewall de última generación Dell SonicWALL, Mobile Connect establece una Clean VPN, una capa de protección adicional que cifra y analiza todo el tráfico SSL VPN, para detectar malware antes de que ingrese a la red.

El firewall de aplicación web y permite el cumplimiento con PCI

El servicio de firewall de aplicación web Dell SonicWALL ofrece a las empresas una solución de cumplimiento completa, asequible e integrada para aplicaciones web que es fácil de administrar e implementar. Admite el cumplimiento con OWASP Top Ten y PCI DSS, lo que proporciona protección contra ataques de inyección y scripts entre sitios (XSS), robo de números de seguridad social y tarjetas de crédito, suplantación de identidad de cookies y falsificación de solicitud entre sitios. Las actualizaciones dinámicas de firmas y las reglas personalizadas ofrecen protección frente a vulnerabilidades conocidas y desconocidas. El firewall de aplicación web puede detectar ataques web sofisticados y proteger aplicaciones web (incluidos portales SSL VPN), denegar el acceso cuando se detecta malware en aplicaciones web y redirigir a los usuarios a una página de error con explicaciones. Proporciona una oferta fácil de implementar con estadísticas y opciones de generación de informes avanzadas con el fin de cumplir con los mandatos de cumplimiento.





❶ Los firewalls Dell SonicWALL de las series NSA o TZ reenvían sin problemas el tráfico entrante al dispositivo Dell SonicWALL SRA, que descifra y autentica el tráfico de red.

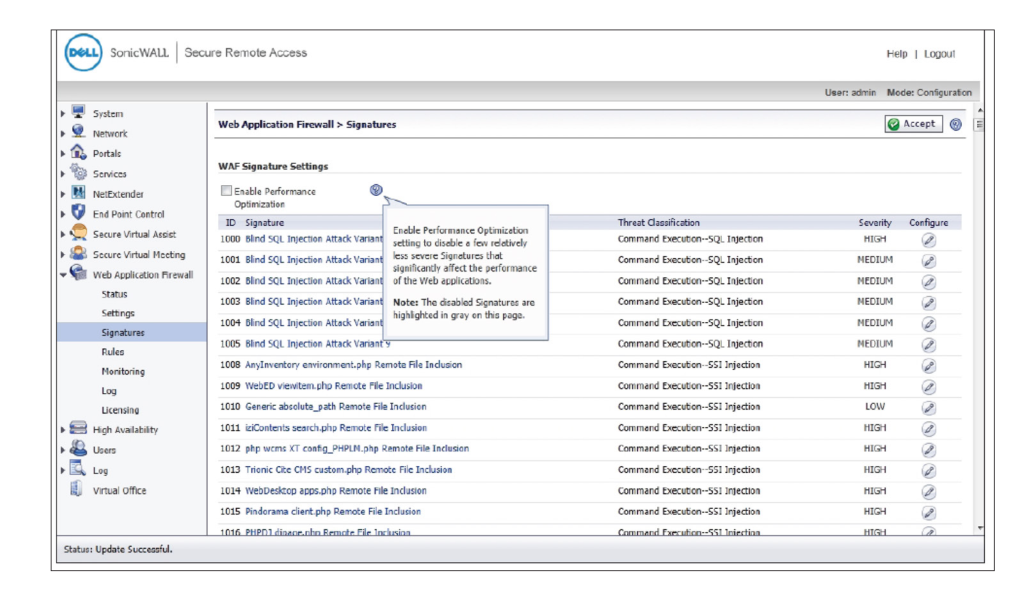
❷ Los usuarios se autentican utilizando una base de datos integrada o mediante métodos de autenticación de terceros, como LDAP, Directorio Activo, Radius, Dell Defender y otras soluciones de autenticación de doble factor.

❸ Un portal web personalizado proporciona acceso únicamente a los recursos para los que el usuario tiene autorización, de acuerdo con las políticas de la compañía.

❹ Para crear un entorno Clean VPN, el tráfico pasa por el firewall de la serie NSA o TZ (que ejecuta antivirus de puerta de enlace, antispyware, prevención de intrusos y control e inteligencia de la aplicación), donde se analiza por completo en busca de virus, gusanos, troyanos, spyware y otras amenazas sofisticadas.

Fácil de administrar

Las soluciones de la serie SRA incluyen política unificada y una interfaz de administración web intuitiva que ofrece ayuda contextual para simplificar el uso. Asimismo, existen varios productos que pueden administrarse de manera centralizada utilizando Dell SonicWALL Global Management System (GMS 4.0+). El acceso a los recursos a través de los productos puede monitorearse sin grandes esfuerzos utilizando la herramienta de generación de informes Dell SonicWALL Analyzer.





Especificaciones

Dell SonicWALL SRA Series

Rendimiento			
	SRA 1600	SRA4600	SRA Virtual Appliance
	Recomendado para organizaciones con 50 empleados o menos	Recomendado para organizaciones con 250 empleados o menos	Recomendado para organizaciones de cualquier tamaño
Licencia de usuarios simultáneos	Comienza con 5 usuarios simultáneos. Licencias de usuarios adicionales disponibles en incrementos de 5 y 10 usuarios.	Comienza con 25 usuarios simultáneos. Licencias de usuarios adicionales disponibles en incrementos de 10, 25 y 100 usuarios.	Licencias de usuario disponibles en incrementos de 5, 10 y 25 usuarios
Capacidad de usuarios1	5 incluidos/50 con licencias/25 recomendados	25 incluidos/500 con licencias/100 recomendados	5 incluidos/50 con licencias
Técnicos de Secure Virtual Assist	Prueba gratuita de 30 días incluida/ máximo de 10 técnicos simultáneos	Prueba gratuita de 30 días incluida/ máximo de 25 técnicos simultáneos	Prueba gratuita de 30 días incluida/ máximo de 25 técnicos simultáneos
Cantidad máxima permitida de participantes de la reunión	–	75	75
Política unificada	Sí. También admite políticas con varios grupos de AD		
Registros	Registros detallados en un formato fácil de leer, alertas por correo electrónico compatibles con Syslog		
Modo de una rama	Sí	Sí	Sí
Dell SonicWALL Secure Virtual Assist o Secure Virtual Access (se obtienen las licencias en conjunto)	Conexión a equipos remotos, chat, FTP y herramientas de diagnóstico y grabación de sesión		
Secure Virtual Meeting2	Agrupa instantáneamente a los participantes de una reunión de manera segura y rentable		
Compatibilidad con IPv6	Básico	Básico	Básico
Equilibrio de carga	Equilibrio de carga HTTP/HTTPS con conmutación por error. Entre los mecanismos se incluyen solicitudes ponderadas, tráfico ponderado, solicitudes menores		
Alta disponibilidad	–	Sí	Sí
Descarga de aplicación	Sí	Sí	Sí
Firewall de aplicaciones web	Sí	Sí	Sí
Control de extremos (EPC)	Sí	Sí	Sí
Políticas basadas en geoubicación4	Sí	Sí	Sí
Filtrado de Botnet4	Sí	Sí	Sí

Características clave	
Aplicaciones admitidas3	• **Acceso de portal web:** Admite HTML5, descarga de proxy y aplicación • **Servicios web:** HTTP, HTTPS, FTP, SSH, Telnet, VNC, Windows® File Sharing (Windows SMB/CIFS), OWA 2003/2007/2010 • **Virtual Desktop Infrastructure (VDI):** Citrix (ICA), RDP • **Mobile Connect y NetExtender:** Cualquier aplicación basada en TCP/IP: ICMP, VoIP, IMAP, POP, SMTP, etc.
Cifrado	ARC4 (128), MD5, SHA-1, SHA-256, SHA-384, SSLv3, TLSv1, TLS 1.1, TLS 1.2, 3DES (168, 256), AES (256), RSA, DHE
Autenticación	Dell Quest Defender, otras soluciones de autenticación de doble factor, contraseñas de única vez, base de datos de usuario interna, RADIUS, LDAP, Microsoft Active Directory e inicio de sesión único (SSO) para la mayoría de las aplicaciones web, RDP y VNC3
Compatibilidad con varios dominios	Sí
Compatibilidad con varios portales	Sí
Control de acceso granular fino	A nivel del usuario, grupo de usuarios y recurso de red
Seguridad de sesión	Los tiempos de expiración por inactividad permiten evitar el uso no autorizado de sesiones inactivas
Certificados	• **Servidor:** Firma propia con nombre común editable e importado de terceros • **Cliente:** Se admiten certificados de cliente opcionales
Limpiador de caché	Configurable. Cuando se cierra la sesión, todas las descargas, las cookies y las URL almacenadas en caché que se descargaron mediante el túnel SSL se eliminan del equipo remoto
Compatibilidad del cliente3	• **Acceso de portal web:** Navegadores Internet Explorer, Mozilla, Chrome, Opera y Safari • **NetExtender:** Windows 2003, 2008, XP/Vista (32 bits y 64 bits), 7 (32 bits y 64 bits), 8 (32 bits y 64 bits), Mac OS X 10.4+, Linux Fedora Core 3+/Ubuntu 7+/OpenSUSE, Linux 64 bits • **Mobile Connect:** iOS 4.2 o posterior, OS X 10.9 o posterior, Android 4.0 o posterior, Kindle Fire con Android 4.0 o posterior y Windows 8.1
Portal personalizado	El usuario remoto puede ver únicamente los recursos para los que el administrador le otorgó acceso de acuerdo con la política de la compañía.
Administración	Interfaz gráfica de usuario web (HTTP, HTTPS), Compatibilidad con SNMP para envío de mensajes syslog y de latidos a GMS (4.0 o posterior)
Monitoreo del uso	Monitoreo gráfico del uso de la memoria, la CPU, los usuarios y el ancho de banda

[1]*La cantidad recomendada de usuarios admitidos se basa en factores como los mecanismos de acceso, las aplicaciones a las cuales se obtiene acceso y el tráfico de las aplicaciones que se envía.*
[2]*Disponible en combinación con Secure Virtual Assist solo para los dispositivos SRA 4600 y SRA Virtual.*
[3]*Consulte las notas de versión de SRA y la guía del administrador más recientes para conocer las configuraciones admitidas.*
[4]*Las políticas de filtrado de Botnet y basadas en geoubicación requieren un contrato de soporte activo en vigencia en el dispositivo virtual o de hardware.*



Hardware		
	SRA 1600	**SRA4600**
Dispositivo de seguridad optimizado	Sí	Sí
Interfaces	(2) Ethernet Gigabit, (2) USB, (1) Consola	(4) Ethernet Gigabit, (2) USB, (1) Consola
Procesadores	Procesador principal x86	Procesador principal x86
Memoria (RAM)	1 GB	2 GB
Memoria flash	1 GB	1 GB
Alimentación de energía/entrada	Interna, 100-240 VCA, 50-60 MHz	Interna, 100-240 VCA, 50-60 MHz
Consumo de energía máximo	47 W	50 W
Disipación de calor total	158,0 BTU	171,0 BTU
Dimensiones	17,00 x 10,13 x 1,75 pulg. 43,18 x 25,73 x 4,45 cm	17,00 x 10,13 x 1,75 pulg. 43,18 x 25,73 x 4,45 cm
Peso del dispositivo	9,50 libras 4,30 kg	9,50 libras 4,30 kg
Peso de la WEEE	10,0 libras 4,50 kg	10,0 libras 4,50 kg
Cumplimiento de las normativas principales	FCC Class A, ICES Class A, CE, C-Tick, VCCI Class A, KCC, ANATEL, BSMI, NOM, UL, cUL, TUV/GS, CB	
Entorno	32-105 ˚F, 0-40 ˚C Humedad: Humedad relativa del 5 % al 95 %, sin condensación	
MTBF	18,3 años	17,8 años
	SRA Virtual Appliance	
Requisitos del entorno virtualizado del dispositivo virtual SRA (mínimo)	Hipervisor: VMWare ESXi y ESX (versión 4.0 o posterior) Tamaño del dispositivo (en disco): 2 GB Memoria asignada: 2 GB	



SRA 1600, 5 usuarios.. **01-SCC-6594**

SRA 1600 usuarios adicionales (50 usuarios máximo)
Adición de 5 usuarios simultáneos.................... **01-SSC-7138**
Adición de 10 usuarios simultáneos.................. **01-SSC-7139**

Soporte de SRA 1600
Soporte dinámico de Dell SonicWALL
24 horas del día, los 7 días de la semana,
hasta 25 usuarios (1 año)....................................... **01-SSC-7141**

Soporte dinámico de Dell SonicWALL
8 horas del día, los 5 días de la semana,
hasta 25 usuarios (1 año)...................................... **01-SSC-7144**



SRA 4600, 25 usuarios.. **01-SSC-6596**

SRA 4600 usuarios adicionales (500 usuarios máximo)
Adición de 10 usuarios simultáneos.................... **01-SSC-7118**
Adición de 25 usuarios simultáneos **01-SSC-7119**
Adición de 100 usuarios simultáneos................. **01-SSC-7120**

Soporte de SRA 4600

Soporte dinámico de Dell SonicWALL
24 horas del día, 7 días de la semana,
hasta 100 usuarios (1 año)...................................... **01-SSC-7123**

Soporte dinámico de Dell SonicWALL
8 horas del día, 5 días de la semana,
hasta 100 usuarios (1 año)...................................... **01-SSC-7126**

Soporte dinámico de Dell SonicWALL
24 horas del día, 7 días de la semana,
de 101 a 500 usuarios (1 año)................................ **01-SSC-7129**

Soporte dinámico de Dell SonicWALL
8 horas del día, 5 días de la semana,
de 101 a 500 usuarios (1 año)................................ **01-SSC-7132**

Dispositivo virtual Dell SonicWALL SRA,
5 usuarios.. **01-SSC-8469**

Usuarios adicionales del dispositivo virtual SRA
(50 usuarios máximo)
Adición de 5 usuarios simultáneos...................... **01-SSC-9182**
Adición de 10 usuarios simultáneos.................... **01-SSC-9183**
Adición de 25 usuarios simultáneos **01-SSC-9184**

Soporte del dispositivo virtual SRA
Soporte dinámico de Dell SonicWALL
8 horas del día, 5 días de la semana,
hasta 25 usuarios (1 año)....................................... **01-SSC-9188**

Soporte dinámico de Dell SonicWALL
24 horas del día, 7 días de la semana,
hasta 25 usuarios (1 año).. **01-SSC-9191**

Soporte dinámico de Dell SonicWALL
8 horas del día, 5 días de la semana,
hasta 50 usuarios (1 año)....................................... **01-SSC-9194**

Soporte dinámico de Dell SonicWALL
24 horas del día, 7 días de la semana,
hasta 50 usuarios (1 año).. **01-SSC-9197**

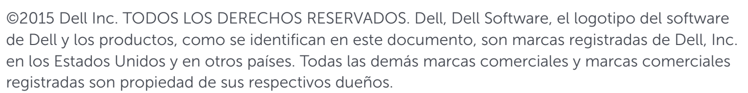
Para obtener más información acerca de las soluciones Dell SonicWALL Secure Remote Access, visite www.sonicwall.com.

Para obtener más información

Dell SonicWALL
5455 Great America Parkway
Santa Clara, CA 95054-3645

www.sonicwall.com
T +1 408.745.9600
F +1 408.745.9300


Software de Dell
5 Polaris Way, Aliso Viejo, CA 92656 | www.dell.com
Si se encuentra fuera de América del Norte, puede encontrar información sobre su oficina local en nuestro sitio web.




DataSheet-SonicWALL-SRASeries-US-VG-25825

